

Vendor Statement of Compliance Data Privacy and Protection

This agreement is entered into between the Roseville City School District ("LEA" or "District") and Super Duper, Inc. ("Service Provider") on 09/30/2022 ("Effective Date").

WHEREAS, the LEA and the Service Provider entered into an agreement for Educational Technology services;

WHEREAS, the LEA is a California public entity subject to all state and federal laws governing education, including but not limited to California Assembly Bill 1584 ("AB 1584"), the California Education Code, the Children's Online Privacy and Protection Act ("COPPA"), and the Family Educational Rights and Privacy Act ("FERPA");

WHEREAS, AB 1584 requires, in part, that any agreement entered into, renewed or amended after January 1, 2015, between a local education agency and a third-party service provider must include certain terms;

NOW, THEREFORE, the Parties agree as follows:

Section I: General - All Data

1. **PASSWORD SECURITY.** All passwords are considered secure. Vendors may not disseminate any passwords unless specifically directed by Educational or Technology Services management. Vendors will not provide information concerning Admin accounts (ROOT Admin, container Admin, local NT administrator or Domain administrator) or their equivalent to any persons. District personnel ONLY will disseminate this information. Vendors will never create "back door" or "generic" user accounts on any systems unless specifically directed to do so by LEA management.

Agree: Yes No

2. **SYSTEM SECURITY.** Unauthorized access to or modification of District systems including file servers, routers, switches, NDS and Internet services is prohibited. Any attempt to bypass or subvert any District security system, both hardware, and software is prohibited.

Agree: Yes No

3. **PRIVACY.** The vendor will adhere to all provisions of the Federal Family Educational Rights and Privacy Act (FERPA, 20 U.S.C. 123g), California Education Code and district policies regarding the protection and confidentiality of data. At all times, the vendor will consider all data collected in the course of their duties to be protected and confidential. Release of this data can only be authorized by Technology & Information Services management and state and federal law.

Agree: Yes No

Section I: General - All Data (Continued)

4. **REUSE:** Vendors shall not copy, duplicate, sell, repackage or use for demonstration purposes any Roseville City School District data without the prior, written consent of Educational or Technology Services management.

Agree: Yes No

5. **TRANSPORT:** Vendor must provide a secure channel (S/FTP, HTTPS, SSH, VPN, etc) for the District to "push" data to the vendor and to extract data as required. Vendors will not have direct access to District systems and will not "pull" data at any time.

Agree: Yes No

6. **EXTERNAL SECURITY:** Vendor must attach to this document reasonable evidence that their system is secure from external hacking and attacks. Devices such as firewalls and technologies such as NAT are the minimum requirements. Active IDS or similar technology is preferred.

Agree: Yes No

7. **INTERNAL SECURITY:** Vendors must attach to this document reasonable evidence that their system is secure from internal hacking and attacks. Describe the interactions vendor personal (or their representatives) will have directly with District data. How is uploaded data from the District handled and processed? Who has access to this data? What happens to the data after the upload is complete? What security safeguards are in place to protected unauthorized access to District data? How are backup performed and who has access to and custody of the backup media? How long are backup maintained; what happens to the District data once the backup is "expired"? If any data is printed, what happens to these hard copy records?

Agree: Yes No

8. **DISTRICT ACCESS:** Vendor must provide a secure means (see Item 5 above) for the District to extract ALL data from the vendor system. This can either be an online extraction tool or a vendor-provided extract as needed by the District (not to exceed quarterly). Describe the means and format of the data (delimited, Excel, MDB, SQL Dump).

Agree: Yes No

9. **TERMINATION:** Upon termination of this agreement as provided herein, the vendor will permanently delete all customer data from their system as allowed by state and federal law. Vendor may be required to certify the destruction of LEA data within 90 days of contract termination.

Agree: Yes No

Section II: AB1584 Compliance - Student Information Only

1. Vendor agrees that the Roseville City School District retains ownership and control of all student data.

Agree: Yes No

2. Vendor must attach to this document a description of how student-created content can be exported and/or transferred to a personal account.

Agree: Yes No

3. Vendor is prohibited from allowing third-parties access to student information beyond those purposes defined in the contract.

Agree: Yes No

4. Vendor must attach to this document a description of how parents, legal guardians and students can review and correct their personally identifiable information.

Agree: Yes No

5. Vendor will attach to this document evidence how student data is kept secure and confidential.

Agree: Yes No

6. Vendor will attach to this document a description of procedures for notifying affected parents, legal guardians or eligible students when there is an unauthorized disclosure of student records.

Agree: Yes No

7. Vendor certifies that student records will not be retained or available to a third party once the contract has expired or is canceled (See Page 2, Item 9).

Agree: Yes No

8. Vendor will attach to this document a description of how they and any third party affiliates comply with FERPA.

Agree: Yes No

9. Vendor and its agents or third parties are prohibited from using personally identifiable information from student records to target advertising to students

Agree: Yes No


Section III: SB 1177 SOPIPA Compliance - Student Information Only

1. Vendors cannot target advertising on their website or any other website using information acquired from students.
Agree: Yes No
2. Vendors cannot create a profile for a student except for school purposes as defined in the executed contract.
Agree: Yes No
3. Vendors cannot sell student information.
Agree: Yes No
4. Vendors cannot disclose student information unless for legal, regulatory, judicial, safety or operational improvement reasons.
Agree: Yes No
5. Vendors must attach to this document evidence of how student information is protected through reasonable security procedures and practices.
Agree: Yes No
6. Vendors must delete district-controlled student information when requested by the District.
Agree: Yes No
7. Vendors must disclose student information when required by law, for legitimate research purposes and for school purposes to educational agencies.
Agree: Yes No

As an authorized representative of my organization, I accept the conditions listed in this document.

Abraham Webber

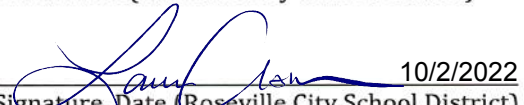
Print Name

 9/30/22

Signature, Date

Laura Assem

Print Name (Roseville City School District)

 10/2/2022

Signature, Date (Roseville City School District)

EXHIBITS

Section 1.6: External Security

Please see attached schedules A&B

Section 1.7: Internal Security

Please see attached schedules A&B

Section II.2: Exporting of Student-Created Content

Please see attached schedules A&B

Section II.4: Review and Correcting Personally Identifiable Information (PII)

Please see attached schedules A&B

EXHIBITS

Section II.5: Securing Student Data

Please see attached schedules A&B

Section II.6: Disclosure Notification

Please see attached schedules A&B

Section II.8: Family Educational Rights and Privacy Act (FERPA) Compliance

Please see attached schedules A&B

Section III.5: How Student Data is Protected:

Please see attached schedules A&B

Super Duper, Inc. dba Super Duper Publications
Data Security and Privacy Plan

Super Duper, Inc. shall maintain Student Data for and on behalf of the District – in accordance with the Family Educational Rights and Privacy Act (“FERPA”), 20 U.S.C. § 1232g(a)(4)(A)(ii), 1232g(b)(1) -- for the purpose of providing HearBuilder Online services (herein “Licensed Product”). Super Duper, Inc. may use the Student Data to conduct collection of metrics to track student progress and performance for teacher reporting activities, including, but not limited to, longitudinal studies, alignment studies, and norming studies for the benefit of the District and/or for the collective benefit of multiple Districts, as permitted by FERPA.

Personally identifiable information ("PII") derived from Student Data provided to Super Duper, Inc. may be disclosed only to Super Duper, Inc. employees who have a legitimate educational interest in maintaining, organizing, or analyzing the data for uses authorized in their Licensed Product. PII derived from Student Data and maintained by Super Duper, Inc. shall not be further disclosed by Super Duper, Inc., except as allowed by FERPA.

Super Duper, Inc. is strongly committed to the privacy of Customers and Students, particularly the privacy of children. Super Duper, Inc. complies with the requirements of the Children's Online Privacy Protection Act of 1998 (COPPA), the Children's Internet Protection Act (CIPA), and FERPA regarding the information collected and maintained by Super Duper, Inc.. Accordingly, we will not collect, use or disclose personal information covered by COPPA, CIPA, and FERPA except in compliance with the respective requirements of each of these statutes and their associated regulations.

With respect to CIPA, Super Duper, Inc.'s Licensed Product is self-contained and does not provide links to external resources or chat rooms. Moreover, HearBuilder Online does not contain any offensive or inappropriate matter. As a result, any school or clinic that uses HearBuilder Online will be fully compliant with CIPA.

We will also comply with all other applicable laws which govern the information maintained by Super Duper, Inc..

Super Duper, Inc. limits access to Protected Data to authorized staff in various ways. Some of these ways include, but are not limited to:

- Super Duper, Inc. employees pass pre-employment background checks.
- Employee roles are separated and monitored logged through password-protected, secure internal network.
- Account access is tailored narrowly to specific roles to limit access to Protected Data. For example, a customer service agent may confirm a password reset request initiated by the Customer, but not able to access Student Data affiliated with said Customer.
- Super Duper, Inc. premises is accessible only through logged key-card access.
- Facilities are monitored 24/7/365 by video surveillance and monitored onsite.

- Access to Protected Data is monitored and logged.
- Super Duper, Inc. is committed to ongoing training, supervision, and assessment of employees so that staff will be trained to be compliant with education laws and demonstrate they understand the depth of their responsibilities according to said laws.
- Training and assessment will take place at a minimum on an annual basis and when changes, if any, occur to relevant federal and state laws.
- At a minimum, Super Duper, Inc. annually reviews its policies and procedures to stay current with federal and state laws regarding data privacy and security.

Below is an outline of how Super Duper, Inc. employs “best practices” and industry standards with respect to data storage, privacy and protection of data:

- Any sensitive online information is transmitted over secure, encrypted channels via SSL as well as other layers of encryption.
- All Student Data is stored on secure servers utilizing encryption and firewall technology and are not publicly accessible.
- All Student performance data is stored in a non-identifiable format.
- Security audits are continuously performed to ensure data integrity.
- Super Duper, Inc. does not share Student Data with any third parties. If a school requests that Student Data should be sent to a third party, Super Duper, Inc. sends the data to the school and never directly to the third party.

Super Duper, Inc. is dedicated to the privacy of children under 13 years of age. We do not process or collect from children more personal information than is needed to access services. The Customer is responsible for obtaining all parental consent necessary for collection of personal information from children under 13. Super Duper, Inc. presumes that such consent has been obtained by Customer by virtue of the Customer having retained Super Duper, Inc. to provide its services.

Parents may review their Student's PII by contacting the Customer. If a request is made to Super Duper, Inc., we will look to the Customer to validate the request and respond accordingly.

Super Duper, Inc. will not share any personal information about children with any third parties other than as specified in this Privacy Policy.

Super Duper, Inc. does not sell, rent, or lease Customer data to third parties. Super Duper, Inc. may share data with trusted partners to help promote safety and security, provide customer support, and to provide the Licensed Product. All such third parties are prohibited from using the Protected Data except to provide these services to Super Duper, Inc., and they are required to maintain the confidentiality of Customer information in compliance with federal and state laws.

Super Duper, Inc.'s web hosting company, Rackspace, Inc. complies with this Data Security and Privacy Plan, and provides a number of additional security measures. These include, but are not limited to, the following:

- Performs pre-employment background screening on all employees with access to Super Duper, Inc. data.
- Restricts administrative access codes specific to Vendor accounts and all activity is logged.
- Agrees to maintain physical, technical, and administrative safeguards defined in the Payment Card Industry-Data Security Standard (PCI-DSS).
- Staffs all data centers 24/7 /365 and monitored by video surveillance and viewed by onsite security force.
- Conducts routine audits and use of electronic access control system which logs access to physical facilities.
- Limits access to physical facilities to authorized individuals by proximity-based access cards and biometric hand scanners.
- Adheres to the best practice standards of ISO 27002; SSAE 16 and ISAE 3402 compliance frameworks; as well as AT 101 compliance framework. The annual SOC reports are reviewed by Super Duper, Inc. and can be made available upon request.
- Reports any material breach of security which results in unauthorized access to Vendor data.

For more information specific to Rackspace, Inc., please consult Rackspace Inc. 's Global Security Practices found here:

<https://www.rackspace.com/information/legal/securitypractices>

Privacy Contact Information

Super Duper, Inc. takes privacy issues very seriously. If you have any questions, suggestions or concerns, please contact us at:

Super Duper, Inc.
ATTN: Privacy Concerns
5201 Pelham Road
Greenville, SC 29615

Phone: 1-800-277-8737

Email: privacy@superduperinc.com